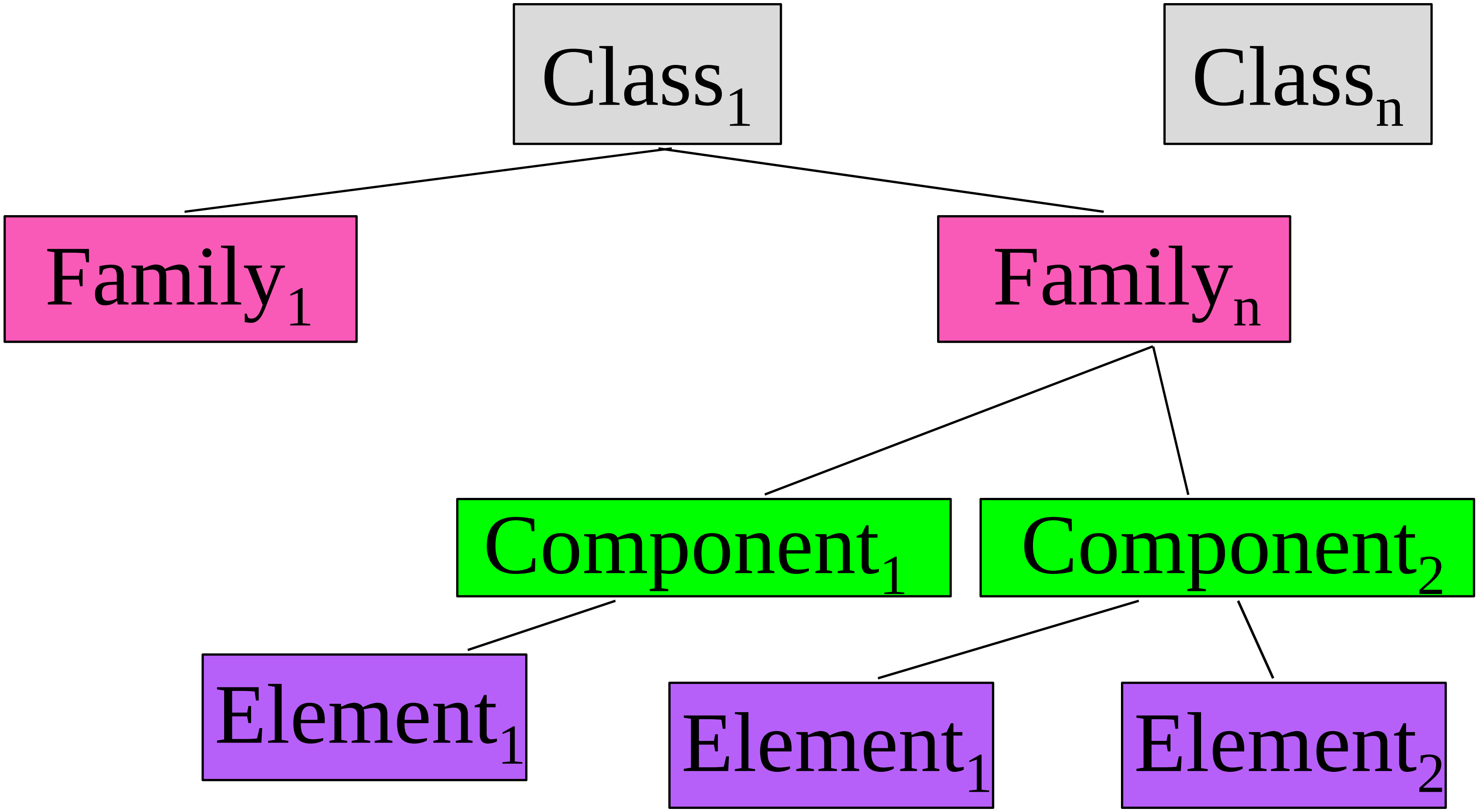
Workshop Schedule
Thursday

- 8am - 9am: Requirements Review
- 9:00am - noon: Requirements Selection Exercise
- noon - 1pm: Lunch
- 1pm - 4pm: Continue Exercise and Prepare Briefings

Security Functional Requirements

Levied upon functions of the TOE that support IT security; their behavior can generally be observed

CC Part 2:
Security Functional Requirements



Don’t Forget About Operations

❑ Selection

❑ Assignment

❑ Refinement

❑ Iteration

❑ Augmentation (EALs)

Requirements Selection Exercise Instructions

❑ You must use the threats, policies, secure usage assumptions and security objectives that have already been defined

❑ Each group will be playing the part of a different entity writing a protection profile and will have a different environment in which to work

Group 1: Government Agency

- **Role:** Food and Drug Administration
- **Portal:** Door to Testing Laboratories
- **Asset(s):** Food/drugs awaiting FDA approval, supporting data, FDA results
- **Value:** High+; could result in bad drug being approved or a good drug not being approved
- **Risk:** High
- **Adversaries:** Competing drug companies
- **Value to adversaries:** High+
- **Resources of adversaries:** Extensive

Goal: Protect assets from tamper.

Group 2: Public Facility

- **Role:** Ronald Reagan National Airport Management
- **Portal:** Entrance to tarmac
- **Asset(s):** Planes (direct), people (indirect)
- **Value:** High+; could result in loss of equipment and lives
- **Risk:** Low - Moderate
- **Adversaries:** Terrorists, criminals
- **Value to adversaries:** Moderate
- **Resources of adversaries:** Moderate

Goal: Protect planes from tamper.

Group 3: Commercial Enterprise (Large Scale)

- ❑ **Role:** MicroSonScape Corporation Management
- ❑ **Portal:** Entrance to Engineering Facility
- ❑ **Asset(s):** Designs, software, tests, etc.
- ❑ **Value:** High; could result in loss of revenue
- ❑ **Risk:** Moderate - High
- ❑ **Adversaries:** Competing companies (numerous software development companies)
- ❑ **Value to adversaries:** High
- ❑ **Resources of adversaries:** Moderate

Goal: Protect assets from disclosure/theft.

Group 4: Commercial Enterprise (Small Scale)

- **Role:** Manager of ATM Machine
- **Portal:** ATM
- **Asset(s):** Customer's money (direct), customer (indirect)
- **Value:** Moderate; could result in loss of customers or customer's money
- **Risk:** High
- **Adversaries:** Criminals
- **Value to adversaries:** Low - moderate
- **Resources of adversaries:** Low

Goal: Protect money from theft.

Functional Requirements Selection Exercise

- ❑ Functional Requirements must include:
  - FIA - Identification and Authentication
  - FAU - Audit
  - FPT - Protection of TSF
  - FMT - Security Management
- ❑ You may also need to select requirements from other classes

Assurance Requirements Selection Exercise

✓ ❶ Value of the “assets”

✓ ❷ Risk of the “assets” being compromised

❸ Current state of practice in definition and construction of Biometric Devices

❹ Development, evaluation, & maintenance costs

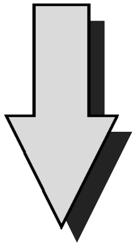
✓ ❺ Resources of adversaries

❻ Functional requirement dependencies

✓ ❼ Security Objectives

Cost of Developing, Evaluating, and Maintaining a Biometric Device

Higher the Assurance Level (EAL)



$$$ Higher the Cost $$$

Biometric Device Definition and Construction:
<u>Current State of Practice</u>

- Configuration Management
- Delivery and Operation
- Product Development

- Guidance Support
- Life Cycle Support
- Testing
- Vulnerability Assessment

Configuration Management
(EAL1 - EAL3)

❑ No vendors use automated CM systems

❑ Most vendors have some type of manual CM system which identifies configuration items and version numbers

❑ Procedures are in place for controlled updates to software and documentation

❑ In general, only software is placed under CM

Delivery and Operation (EAL1 - EAL3)

- ❑ Good documentation for secure installation and start-up is generally available
- ❑ Some vendors provide on-site installation
- ❑ Delivery procedures are documented and followed

Product Development (EAL1 - EAL2)

- Documentation available that describes:
  - user interface
  - security functions (functional specification)
- All documentation is informal
- High-level design docs exist and cover major subsystems & their interfaces
- Schematics of hardware components sometimes available
- Mapping between the functional spec and the high-level design does exist but not very detailed

Guidance Support
(EAL1 - EAL7)

- ❑ Administrator documentation good
- ❑ User documentation is limited or non-existent
- ❑ Rationale could explain the failure to meet AGD_USR.1

Life Cycle Support (EAL1 - EAL2)

❑ No vendor uses a specific life-cycle model for development & maintenance

❑ Development toolkits are used

❑ Implementation standards are generally only used by ISO 9000 compliant vendors

Testing
(EAL1)

- ❑ Test coverage analysis not routinely performed by any vendor
- ❑ Testing is rigorous and done at several levels:
  - – performance testing internally
  - – customer performance testing
  - – independent testing

Vulnerability Assessment (EAL1)

- Covert channel analyses never done
- Direct attacks are simulated for penetration testing

Current State of Practice Summary

❑ Configuration Management	EAL1 - EAL3
❑ Installation,Generation,Start-Up	EAL1 - EAL3
❑ Product Development	EAL1 - EAL2
❑ Guidance Support	EAL1 - EAL7
❑ Life Cycle Support	EAL1 - EAL2
❑ Testing	EAL1
❑ Vulnerability Assessment	EAL1

Group Briefings

❏ 5-10 minute briefing

❏ Focus on:

- <u>Rationale</u> for functional requirements
- <u>Rationale</u> for assurance requirements
- Interesting/unique requirements selected
- Problems and how your group solved them

❏ 10-15 minute question/answer period

Workshop Schedule
Friday

- 8am - 10am: Finish Preparing Briefings
- 10am - noon: Briefings & Discussion
- 12pm - 1pm: Lunch
- 1pm - 3pm: Panel - Window into the Future
- 3pm - 4pm: Comments from the Class